The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

12/10/2013

SUBJECT:

Multiple Vulnerabilities in Microsoft Exchange Server Could Allow Remote Code Execution (MS13-105)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft Exchange Server. Microsoft Exchange Server is an email server software product from Microsoft. This vulnerability can be exploited when a user opens a specially crafted email in Outlook Web Access (OWA). Successful exploitation could allow an attacker to gain the same privileges as a local server account. Depending on the privileges associated with the account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Exchange Server 2007
- Exchange Server 2010
- Exchange Server 2013

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:

Multiple vulnerabilities have been discovered in Microsoft Exchange Server that could allow a remote attacker to take control of a service account on an Exchange Server. Details of these vulnerabilities are as follows:

Oracle Outside In Contains Multiple Exploitable Vulnerabilities - CVE-2013-5763 and CVE-2013-5791

Two of the vulnerabilities addressed in this bulletin, CVE-2013-5763 and CVE-2013-5791, exist in Exchange Server 2007, Exchange Server 2010, and Exchange Server 2013 through the WebReady Document Viewing feature. The vulnerabilities could allow remote code execution as the LocalService account if a user views a specially crafted file through Outlook Web Access in a browser. An attacker who successfully exploited this vulnerability could run code on the affected Exchange Server, but only as the LocalService account. The LocalService account has minimum privileges on the local computer and presents anonymous credentials on the network.

In addition, CVE-2013-5763 and CVE-2013-5791 exist in Exchange Server 2013 through the Data Loss Protection (DLP) feature. This vulnerability could cause the affected Exchange Server to become unresponsive if a user sends or receives a specially crafted file.

MAC Disabled Vulnerability – CVE-2013-1330

A remote code execution vulnerability exists in Microsoft Exchange Server. This vulnerability is caused due to Exchange Server not properly validating input. This vulnerability can be exploited if an attacker sends specially crafted content to a target server. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the Outlook Web Access (OWA) service account.

OWA XSS Vulnerability – CVE-2013-5072

An elevation of privilege vulnerability exists in Microsoft Exchange Server. This vulnerability can be exploited if a user opens a specially crafted URL that takes the user to a targeted Outlook Web Access site. An attacker who successfully exploited this vulnerability could then run a script in the context of the current user.

Successful exploitation of these vulnerabilities could allow an attacker to gain the same privileges as a local account. Depending on the privileges associated with the account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Microsoft:

http://technet.microsoft.com/en-us/security/bulletin/ms13-105

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5763

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5791

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1330

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5072